Trust Assessment in Vehicular Social Network based on Three-Valued Subjective Logic

Tong Cheng, Guangchi Liu, Qing Yang, *Senior Member, IEEE,* and Jianguo Sun, *Member, IEEE*

***Abstract*—Trustworthiness in vehicular network plays a vital role in facilitating data sharing among vehicles, to achieve better driving safety and convenience. Without trustworthiness assessment, a vehicle may not be able to trust other vehicles, and therefore simply drop the data shared from others, to avoid potential driving dangers. This problem was traditionally approached by protecting data security, however, the study of the trustworthiness of data generators (vehicles) is unfortunately omitted. We envision the existences of a vehicular social network on road, wherein vehicles exchanging data between each other are considered socially connected. Leveraging the trust propagation and fusion within a vehicular social network, the trustworthiness of individual vehicles can be accurately assessed. We adopt the three-valued subjective logic model to study trust between vehicles, and propose a holistic solution to trust assessment in vehicular social networks. The proposed solution enables objective and subjective trust assessment of vehicles, in a distributed manner. Simulation results indicate that the proposed solution offers a more accurate trust assessment and a quicker assessing time.**

***Index Terms*—Trust assessment, vehicular social network, three-valued subjective logic, community division, distributed algorithm.**

I. Introduction

The current transportation system is going through a revolution with the rapid development of connected and autonomous vehicle (CAV) technologies [1], enabled by the new sensor advancements and wireless communication techniques. According to the recent report released by Cisco [2], 400 million gigabytes of data will be generated by current passenger vehicles, if they are interconnected via wireless technologies. Notably, most of these data are generated by sensors on CAVs. Unlike existing intelligent transportation systems that heavily rely on roadside infrastructures (e.g., camera, Doppler radar, embedded sensors), CAVs provide more accurate and timely information, e.g., traffic volume and road conditions, within a larger area. By utilizing the data shared from other vehicles, a vehicle is able to broaden its sensing range and has a better perception about its surrounding environment.

Because data are collected by individual vehicles, equipped with various types of sensors and data processing algorithms, the trustworthiness of data cannot be guaranteed. In other words, untrustworthy information may be generated and exchanged between vehicles and/or roadside infrastructures. Information trustworthiness is different from security as even a vehicle under strong security protection can still generate untrustworthy information, e.g., due to hardware or software defects. Without the knowledge about the trustworthiness of data exchanged from other vehicles, a vehicle may have to drop the data as it is too risky to blindly trust the received data. As the safety of connected vehicular systems largely depends on trustworthy data sharing, it is critical to enable a vehicle to assess in real time the trustworthiness of other vehicles, as well as their generated data.

A. Proposed Approach

Existing research on trustworthy vehicular systems mainly focuses security, i.e., guaranteeing a vehicular system's confidentiality, integrity, and authentication. However, it is not clear how to assess the trustworthiness of the data and/or the data generators (vehicles). To tackle this problem, we treat the event of sharing data between vehicles as a social interaction (between them), and model a vehicular network as a social network. Within this network, vehicles are considered to be "socially" connected if and only if they exchanged data between each other. Based on the quality and quantity of their interactions, vehicles are able to evaluate the trustworthiness of each other. When a vehicle receives data from another vehicle, it evaluates the trustworthiness of the data by comparing them to its own sensing results. The vehicle tends to trust those providing similar sensing data, while distrust others. As such, an trust opinion is formed, which is called the direct trust/opinion as it is derived from the direct interactions between vehicles. If a vehicle does not directly interact with another vehicle, it will leverage its own social connections to infer the (indirect) trust of that vehicle.

Given a vehicular social network, we first assume the network is static, i.e., the topology are not changing, and propose the OpinionWalk algorithm to infer the indirect trust between vehicles. In the OpinionWalk algorithm, we use an opinion matrix to represent the topology of a vehicular social network. Each entry in the opinion matrix indicates a direct relation between two vehicles, if they exchanged data between each other. Here, we adopt the three-valued subjective logic (3VSL) to model the trust between vehicles [3]. Then, a set of matrix-like operations are designed, i.e., the traditional multiplication and summation operations in matrix multiplication are replaced by the discounting and combining operations

T. Cheng and Q. Yang are with the Department of Computer Science and Engineering, University of North Texas, Denton, Texas 76203, USA Emails:{tong.cheng, qing.yang}@unt.edu.

G. Liu is with the Stratifyd Inc., Charlotte, NC 28207, USA. Email:luke.liu@stratifyd.com.

J. Sun is with the College of Computer Science, Harbin Engineering University, Harbin, Heilongjiang, 150001, China. Email:sunjianguo@hrbeu.edu.cn.

Q. Yang is the corresponding author of this article.

Manuscript received xx; revised xx.

on trust relations. The discounting and combining operations were defined in the 3VSL model, and used to model trust propagation and fusion in a social network. Based on these operations, OpinionWalk starts from a vehicle and searches its social network to infer the trustworthiness of other vehicles, in an iterative manner.

One of the major challenges faced in vehicular networks is the dynamic network topology due to the rapid changes in vehicular speeds. Similarly, the interactions between vehicles occur only when they encounter with each other on the road. As a matter of fact, the highly dynamic nature of a vehicular social network poses both challenges and opportunities to trust assessment of vehicles. It becomes an undesirable difficulty in trust assessment as trust assessment algorithms need to be re-executed, whenever a change occurs within the network. On the other hand, as a vehicle encounters and interacts with more vehicles, it has the opportunity to connect to some very trustworthy ones, thus receiving more trustworthy and valuable information from them. Based on the data sent from the trustworthy ones, a vehicle can accurately estimate its own trustworthiness. With an accurate self-evaluation, the vehicle is able to better estimate the trustworthiness of other (untrustworthy) vehicles. As vehicles usually move on regular routes, e.g., commuters usually drive between their homes and offices, those with similar routes could be grouped into one community as they frequently interact with each other. The size of a community is usually much smaller than that of the entire vehicular social network, therefore, trust assessment can be done within communities to reduce the trust computation overhead. We propose both static and dynamic trust computation mechanisms to deal with the trust assessment problem in vehicular networks.

B. Key Contributions

The key contributions of this paper are concluded as follows. We consider the data exchange between vehicles as a form of interaction and construct a vehicular social network to reflect the social relations/connections among vehicles. For a vehicular social network, we design the OpinionWalk algorithm to accurately assess the subjective trust of individual vehicles, leveraging the three-valued subjective logic (3VSL) trust model. By investigating the quality of data exchanged among vehicles, we design a mechanism to conduct the objective trust assessment, which is proven to be more accurate than subjective trust assessment. Finally, we treat vehicles in groups/communities and propose a solution to intra-community and inter-community trust assessments. Simulation results demonstrate the accuracy and efficiency of the proposed solution.

The paper is organized as follows. In Section II, the background and preliminaries are presented. Based on the three-valued subjective logic model, the OpinionWalk algorithm is introduced in Section III. To deal with the dynamics of a vehicular social network, a dynamic trust assessment method is proposed in Section IV. The proposed holistic solution is validated and evaluated in Section V. Section VI gives the related work on vehicular social network and trust assessment in online social networks. Finally, Section VII concludes the work.

II. Preliminaries

A. 3VSL Trust Model

Three-Valued Subjective Logic (3VSL) model was introduced to accurately model interpersonal trust between users in online social networks, and it was proven to be applicable in social networks with arbitrate typologies [3]. The 3VSL model is adapted in this paper to capture the trust relations between vehicles. Trust between vehicles is built upon the interactions between them, e.g., when they exchange data between each other. Given that vehicle i receives data from vehicle j and tries to evaluate j's trust, we call vehicle i as the trustor, j as the trustee, and the evaluating process as the trust assessment. Given trustor i and trustee j, i's opinion about j's trust can be represented as

$$\omega_{ij} = (b_{ij}, d_{ij}, n_{ij}, e_{ij}),$$

where $b_{ij} + d_{ij} + n_{ij} + e_{ij} = 1$. Here, b_{ij}, d_{ij}, n_{ij} represent the *posterior* probabilities that the data generated from vehicle j are trustworthy, untrustworthy, or uncertain, from vehicle i's perspective. e_{ij}, on the other hand, represents the *prior* probability that the data are trustworthy, untrustworthy or uncertain.

Specifically, given the amount of trustworthy, untrustworthy, or uncertain data observations generated from vehicle as r, s and o, we have

$$\begin{cases} b_{ij} = \dfrac{r_{ij}}{r_{ij} + s_{ij} + o_{ij} + 3} \\ d_{ij} = \dfrac{s_{ij}}{r_{ij} + s_{ij} + o_{ij} + 3} \\ n_{ij} = \dfrac{o_{ij}}{r_{ij} + s_{ij} + o_{ij} + 3} \\ e_{ij} = \dfrac{3}{r_{ij} + s_{ij} + o_{ij} + 3} \end{cases}.$$

Note that ω_{ij} only represents i's subjective opinion about j's trust, which is different from j's objective trust, which will be introduced later. The values of r_{ij}, s_{ij} and o_{ij} are determined by the quality and quantity of interactions between vehicles i and j. For example, if vehicle j shares 7 pieces of information to vehicle i. If i determines that 3 pieces of them are trustworthy, 2 pieces are not trustworthy, and 2 piece is uncertain, then $r_{ij} = 3$, $s_{ij} = 2$, and $o_{ij} = 2$. Here, e_{ij} represents prior uncertainty, which always comes from 3 prior observations for trustworthy, not trustworthy and uncertain, respectively. As a result, we have $b_{ij} = 0.4$, $d_{ij} = 0.3$, and $j_{ij} = 0.3$. Notably, the same 10 pieces of data might be viewed differently by another vehicle, due to the subjectivity of trust.

If vehicles i and j has no interaction, then i holds an uncertain opinion about j's trust, $\omega_{ij} = \mathbb{O}$. The *uncertain* opinion $\mathbb{O}$ is defined as $(0, 0, 0, 1)$, indicating $r = s = o = 0$, i.e., a trustor is totally uncertain about a trustee's trust. In other words, his trust is based on the 3 prior observations only.

Although i has no direct opinion on j, it might derive an indirect opinion on j, e.g., via others' recommendations. We use Ω_{ij} to denote i's indirect opinion on j. It is well-known that trust can propagate and fuse within social networks [4]. To model trust propagation and fusion in online social networks,

3VSL defines the *discounting* and *combining* operations as follows. The discounting operation $\Delta(\omega_{is}, \omega_{sj})$ is used to compute i's opinion about j's trust, based on s's recommendation on j, where s is a mutual friend between i and j. The discounting operation yields a new indirect opinion Ω_{ij} where

$$\begin{cases} b_{ij} = b_{is}b_{sj} \\ d_{ij} = b_{is}d_{sj} \\ n_{ij} = 1 - b_{ij} - d_{ij} - e_{sj} \\ e_{ij} = e_{ij} \end{cases}.$$

The combining operation $\Theta(\omega'_{ij}, \omega''_{ij})$ is used to fuse i's two opinions on j's trust. The combining operation generates a new opinion Ω_{ij} where

$$\begin{cases} b_{ij} = \dfrac{e''_{ij}b'_{ij} + e'_{ij}b''_{ij}}{e'_{ij} + e''_{ij} - e'_{ij}e''_{ij}} \\ d_{ij} = \dfrac{e''_{ij}d'_{ij} + e'_{ij}d''_{ij}}{e'_{ij} + e''_{ij} - e'_{ij}e''_{ij}} \\ n_{ij} = \dfrac{e''_{ij}n'_{ij} + e'_{ij}n''_{ij}}{e'_{ij} + e''_{ij} - e'_{ij}e''_{ij}} \\ e_{ij} = \dfrac{e'_{ij}e''_{ij}}{e'_{ij} + e''_{ij} - e'_{ij}e''_{ij}} \end{cases}.$$

B. Trust Assessment in Vehicular Social Network

A vehicular social network is modeled as a directed graph $G(V, E)$ where a vertex $i \in V$ represents a vehicle, and an edge $e(i, j)$ indicates that vehicle i receives data from vehicle j [5]. By checking whether the received data is trustworthy, vehicle i is able to derive its own opinion about j's trust, denoted as ω_{ij}. As such, a trust vehicular social network can be formed, denoted as $G(V, E, \omega)$, in which the weight of edge $e(i, j)$ is denoted as ω_{ij}.

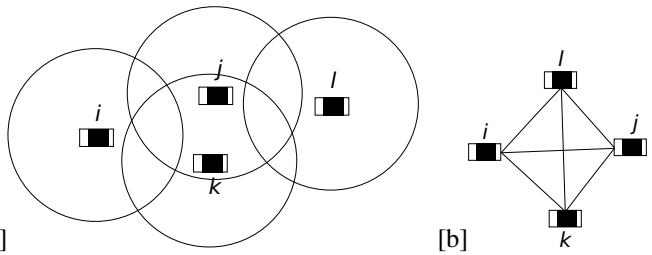


Fig. 1. Data sharing among vehicles fosters the construction of a local vehicular social network.

As shown in Fig. 1(a), let's assume four vehicles i, j, k, l are within the communication range of each other. For the sake of better representation, the communication range of each vehicle is not shown in this figure. The circles in the figure represent the sensing ranges of individual vehicles, which is much smaller than the communication range. We assume vehicle i is the trustor and it tries to compute the trust of all other vehicles. To do so, it needs to evaluate the trustworthiness of the sensing data shared by other vehicles. As such, vehicle i will build a social network to record its connections to other vehicles, as shown in Fig. 1(b). The weight of each edge is derived from evaluating the trustworthiness of the sensing data sent from corresponding vehicles, which will be discussed later.

For any vehicle on road, if it receives information from others, it needs to quickly decide whether the sender is trustworthy. If the information is shared from a trustworthy vehicle, it will fuse the received data into its decision making module; otherwise, it will simply discard the data. The problem of trust assessment in a vehicular social network can then be formulated as follows. Given a trust vehicular social network $G(V, E, \omega)$, $\forall$ i and j, s.t. $i, j \in V$, $\exists$ at least one path from i to j, how to compute i's trust in users $\{j \in V, j \neq i\}$. The proposed problem can be solved in two steps. In the first step, a static graph $G(V, E, w)$ is assumed and the OpinionWalk algorithm is proposed to address this problem. In the second step, the graph $G(V, E, w)$ is dynamic as vehicles move on road, so we propose a dynamic trust assessment algorithm to tackle the problem.

III. Static Trust Assessment

Assuming graph $G(V, E, w)$ is static, we design the OpinionWalk algorithm[1] to compute a vehicle i's trust in all other vehicles within its social network. The OpinionWalk algorithm is essentially a breadth first search (BFS) based algorithm that computes the trust of all other vehicles that are indirectly connected to i. In the extreme case where vehicle i is directly connected to only one vehicle and indirectly connected to all other vehicles, the OpinionWalk algorithm needs to search the entire network, represented by graph $G(V, E, w)$, to compute i's trust in all other vehicles. Apparently, OpinionWalk is slow for trust assessment in this case; therefore, we propose to divide vehicles into communities and apply OpinionWalk in each community to speed up the trust assessment (in Section IV).

Given a vehicular social network $G(V, E, w)$ where $|V| = n$, OpinionWalk represents G as an opinion matrix

$$M = \begin{bmatrix} \omega_{11} & \omega_{12} & \dots & \omega_{1n} \\ \omega_{21} & \omega_{22} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \omega_{n1} & \cdots & \cdots & \omega_{nn} \end{bmatrix},$$

where an element ω_{ij} $(i, j \leq n)$ denotes vehicle i's direct opinion on j's trust. If vehicle i has no direct interaction with j, we use $\mathbb{O}$ to denote the opinion $\omega_{ij} = \mathbb{O}$.

From the trustor i's perspective, its opinions on the trust of all other vehicles are stored in the *individual opinion vector*

$$Y_i^{(k)} = \left[\Omega_{i1}^{(k)}, \Omega_{i2}^{(k)}, \cdots, \Omega_{ij}^{(k)}, \cdots, \Omega_{in}^{(k)}\right]^{\mathrm{T}},$$

where $\Omega_{ij}^{(k)}$ denotes i's opinion on j's trust, after OpinionWalk algorithm "walks" k levels on the graph G. The individual opinion vector is initialized as

$$\Omega_{ij}^{(1)} = \begin{cases} \omega_{ij}, \text{ if vehicles } i \text{ and } j \text{ have interactions} \\ \mathbb{O}, \text{ otherwise} \end{cases}.$$

As such, when OpinionWalk searches the graph G, the individual opinion vector is updated as follows.

$$Y_i^{(k)} = M^T \odot Y_i^{(k-1)}. \quad (1)$$

[1]The preliminary version of the OpinionWalk algorithm was published in IEEE INFOCOM 2017 [6]

A. Operations in OpinionWalk

Before we detail the operations defined in Eq. 1, let's introduce the intuition of operator $\odot$ in Fig. 2. In the figure, OpinionWalk starts from vehicle i and searches i's social network level by level. Suppose OpinionWalk is currently searching the $(k-1)$-th level, and it finds a set of vehicles that are $(k-1)$-hop away from i. Among these vehicles, we assume m of them directly connect to j, i.e., j is k-hop away from i. We label them as $s_1, s_2, \cdots, s_m$.

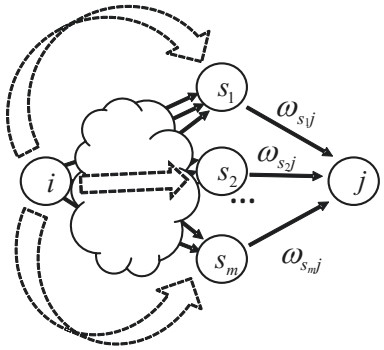


Fig. 2. Illustration of the principle of the $\odot$ operator in OpinionWalk.

When OpinionWalk moves to the next level, i.e., the k-th level, it updates i's opinion on j to

$$\Theta\left(\Delta(\Omega_{is_1}^{(k-1)}, \omega_{s_1 j}), \cdots, \Delta(\Omega_{is_m}^{(k-1)}, \omega_{s_m j})\right),$$

where Θ and Δ are the combining and discounting operations, defined in 3VSL [3]. The formula essentially combines all m indirect opinions computed from discounting $\omega_{s_l j}$ by Ω_{is_l}, for all possible $l = 1, 2, \cdots, m$. It is proven that equation[2] can be further generalized into

$$\Theta\left(\Delta(\Omega_{i1}^{(k-1)}, \omega_{1j}), \cdots, \Delta(\Omega_{in}^{(k-1)}, \omega_{nj})\right). \quad (2)$$

It is possible that $\Omega_{ij}^{(k-1)} \neq \mathbb{O}$, i.e., OpinionWalk already obtains i's opinion on j's trust in the previous search(es). Then, i's opinion on j will be replaced with $\Omega_{ij}^{(k)}$. In other words, only the opinions $\Omega_{is}^{(k-1)}$ for $\omega_{sj} \neq \mathbb{O}$ are used in updating the individual opinion vector.

Based on the updating process, we can use a matrix-like operation to formalize Eq. 1, where the operator $\odot$ "multiplies" matrix M and vector $Y_i^{(k-1)}$ to yield a new vector $Y_i^{(k)}$ as follows.

$$\begin{aligned} Y_i^{(k)} &= M^T \odot Y_i^{(k-1)} \\ &= \begin{bmatrix} \Theta\left(\Delta(\Omega_{i1}^{(k-1)}, \omega_{11}), \cdots, \Delta(\Omega_{in}^{(k-1)}, \omega_{n1})\right), \\ \Theta\left(\Delta(\Omega_{i1}^{(k-1)}, \omega_{12}), \cdots, \Delta(\Omega_{in}^{(k-1)}, \omega_{n2})\right), \\ \cdots \\ \Theta\left(\Delta(\Omega_{i1}^{(k-1)}, \omega_{1n}), \cdots, \Delta(\Omega_{in}^{(k-1)}, \omega_{nn})\right) \end{bmatrix} \\ &= \left[\Omega_{i1}^{(k)}, \Omega_{i2}^{(k)}, \cdots, \Omega_{ij}^{(k)}, \cdots, \Omega_{in}^{(k)}\right]^{\mathrm{T}}. \end{aligned}$$

[2]The equation here is generalized for better presentation; however, when it is implemented, only m opinions are considered.

As shown in Fig. 3, the function of $\odot$ is analogous to the multiplication between a matrix and a vector. The difference

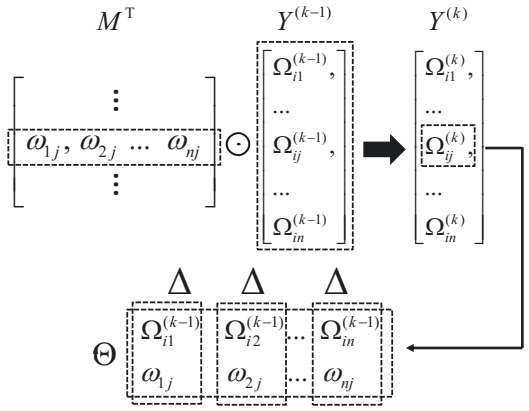


Fig. 3. A diagrammatic overview of the $\odot$ operation in OpinionWalk.

lies in the summation and multiplication operations are replaced with the combining and discounting operations defined in 3VSL, respectively.

Let's look at the element $\Omega_{ij}^{(k)}$ in $Y_i^{(k)}$ where $i \neq j$. It is computed by "multiplying" vectors $\left[\omega_{1j}, \omega_{2j}, \cdots, \omega_{nj}\right]$ and $\left[\Omega_{i1}^{(k-1)}, \Omega_{i2}^{(k-1)}, \cdots, \Omega_{in}^{(k-1)}\right]^{\mathrm{T}}$. It is worth mentioning that the opinion matrix M can be used by any vehicle to compute its opinion about the trust of all other vehicles in the network. However, every single trustor needs an individual opinion vector to store its own opinion about the trust of all others.

B. OpinionWalk Algorithm

Algorithm 1 OpinionWalk(G, i, H)

Require: A directed graph G with a trustor i and the maximum searching level H.
Ensure: i's opinion j where $j \neq i$.

```
1:  Initialize M and Y_i^(1) based on G
2:  k ← 1
3:  while k < H do
4:      k ← k + 1
5:      for all columns c_j ∈ M s.t. j ≠ i do
6:          Ω_ij^(k) ← 𝕆
7:          for all direct opinions ω_sj ∈ c_j s.t. ω_sj ≠ 𝕆 do
8:              Ω_is^(k-1) ← Y_i^(k-1)[s]
9:              if Ω_is^(k-1) ≠ 𝕆 then
10:                 Ω_ij^(k) ← Θ(Ω_ij^(k), Δ(Ω_is^(k-1), ω_sj))
11:             end if
12:         end for
13:         Y_i^(k)[j] ← Ω_ij^(k)
14:     end for
15: end while
16: return Y_i^(k)
```

The pseudo-code of OpinionWalk algorithm is shown in Algorithm 1. In the algorithm, line 3 controls how many hops OpinionWalk will "walk" in the network. Lines 5-14

update the indirect opinion Ω_{ij} iteratively. Line 5 considers all vehicles, other than vehicle i, as the trustees. Lines 7-12 combine all opinions derived from $\omega_{sj} \neq \mathbb{O}$. Line 8 obtains i's indirect opinion on one of the predecessors of j, e.g., s. If this opinion already exists, i discounts s's opinion on j to update $\Omega_{ij}^{(k)}$ at line 9. Otherwise, it checks another predecessor. Line 10 combines all opinions that are computed from $\omega_{sj} \neq \mathbb{O}$. Note that line 10 essentially combines opinions one by one, so $\Omega_{ij}^{(k)}$ equals to

$$\Theta(\Delta(\Omega_{i1}^{(k-1)}, \omega_{1j}), \cdots, \Theta(\Delta(\Omega_{in-1}^{(k-1)}, \omega_{n-1j}), \Delta(\Omega_{in}^{(k-1)}, \omega_{nj}))).$$

Because the combining operation is associative [3], the above equation is the same as Eq. 2. After processing all vehicles connecting to j, at line 13, the newly computed Ω_{ij} is used to update the corresponding element in the individual opinion vector Y_i. When i's opinions on all possible j's are updated, at line 14, OpinionWalk moves to the next level. Finally, the vector $Y_i^{(k)}$ will contain i's opinions about the trust of all other vehicles.

In the OpinionWalk algorithm, there are two nested loops, and the number of iterations in each loop is $O(n)$, so the time complexity of the nested loops is $O(n^2)$. The parameter H indicates the maximum searching depth in the graph, which is usually a constant number, so the OpinionWalk's time complexity becomes $O(n^2)$.

IV. Dynamic Trust Assessment

As vehicles move on road, not only the topology but also the weights of edges in a vehicular social network frequently change. Therefore, it is essential to design a trust assessment mechanism that handles the dynamics of a vehicular social network. In this section, we first show how a single vehicle assesses the trust of another vehicle, if they exchanged data between each other. Then, we leverage the OpinionWalk algorithm to compute the trust of vehicles that have no direct interactions. To achieve efficient indirect trust assessment, vehicles are divided into communities, and the OpinionWalk algorithm is only applied in individual communities to achieve intra-community and inter-community trust assessments.

A. Direct Trust Assessment

Given two vehicles i and j, let's assume there exists an overlapping area x_{ij} between their sensing zones. We assume there are m_{ij} objects in the area x_{ij}. The object here refers to anything that is detectable by a vehicle's sensors. It could be a vehicle, a pedestrian, a cyclist, or a road sign. In the following, we will illustrate how a vehicle conducts subjective and objective trust assessments of another vehicle, based on its own sensing data.

1) Direct Subjective Trust Assessment: For an object in x_{ij}, it could be detected by vehicle i with a certain probability, denoted as p_i. The probability can be assumed to follow a Gaussian distribution, i.e., $p_i \sim \mathcal{N}(b_i, \sigma_i^2)$, where b_i and σ_i denote the mean and standard deviation. Here, b_i indicates the probability that vehicle i is trustworthy, in terms of detecting objects.

As vehicles i and j sense the objects from different locations and/or angles, they may or may not agree upon their sensing results. For example, an object may be detected as a pedestrian by i but a cyclist by j. We use r_{ij} and s_{ij} to denote the numbers of objects that i and j agree and disagree upon, respectively. As such, vehicle i builds its own opinion about the trust of j, regarding to j's ability of detecting objects. We denote this opinion as $\omega_{ij} = (b_{ij}, d_{ij}, 0, e_{ij})$ where

$$\begin{cases} b_{ij} = \dfrac{r_{ij}}{r_{ij} + s_{ij} + 3} \\ d_{ij} = \dfrac{s_{ij}}{r_{ij} + s_{ij} + 3} \\ e_{ij} = \dfrac{3}{r_{ij} + s_{ij} + 3} \end{cases}. \tag{3}$$

As vehicle j uses the same numbers $r_{ji} = r_{ij}$ and $s_{ji} = s_{ij}$ to compute vehicle i's trustworthiness, we have $\omega_{ij} = \omega_{ji}$.

From opinion $\omega_{ij} = (b_{ij}, d_{ij}, 0, e_{ij})$, we can calculate the expected belief of the opinion as [7]

$$E(\omega_{ij}) = \frac{r \cdot c + 0.5(r+s)(1-c)}{r+s}, \tag{4}$$

where c is used to measure the certainty of a probability density function

$$c = \frac{1}{2} \int_0^1 \left| \frac{x^r(1-x^s)}{\int_0^1 x^r(1-x)^s \mathrm{d}x} - 1 \right| \mathrm{d}x. \tag{5}$$

Here, the expected belief $E(\omega_{ij})$ represents i's subjective trust in j. By checking the sensing data sent from j, vehicle i is able to compute the subjective trust of j. Because the trust is generated from vehicles exchanging sensing data to each other, we call it direct subjective trust.

2) Direct Objective Trust Assessment: A vehicle (trustor) forms a subjective trust opinion of another vehicle (trustee), based on the difference between their sensing data, so the opinion may not accurately reflect the trustee vehicle's objective trust. In other words, a subjective opinion only tells how different a trustor and a trustee is, it cannot be directly used as the trustee's trustworthiness. In this section, we introduce a mechanism to dynamically estimate a vehicle's objective trust.

As shown in the Fig. 1(b), among vehicle i's neighbors, we first identify the pair of vehicles whose direct trust values are above a certain threshold t^*. In the figure, vehicle i has the following trust opinions: ω_{ij}, ω_{ik}, and ω_{jk}. If there are enough neighbors, i can always find these vehicles. Assume vehicles j and k are one pair of these nodes, and they make independent observations of the objects in x_{jk}, we have

$$\begin{cases} r_{jk} = m_{jk}\left(p_j p_k + (1-p_j)(1-p_k)\right) \\ s_{jk} = m_{jk} - r_{jk} \end{cases}, \tag{6}$$

where m_{jk} is the total number of objects observed by both vehicles j and k.

For autonomous driving vehicles, we assume their probability of successfully detecting objects are greater than 50%. According to the literature, the probability ranges from 60% to 90% [8], depending on the types of sensors and processing algorithms. If p_j and p_k are within $[60\%, 90\%]$, we know the value of $\left(p_j p_k + (1-p_j)(1-p_k)\right)$ increases as p_j and p_k

increase. In other words, if $E(\omega_{jk})$ is larger than t^*, it means $\big(p_j p_k + (1-p_j)(1-p_k)\big)$ is greater than a certain value, so does the p_j and p_k. As such, the chosen vehicles j and k tend to be more trustworthy than the other neighbors.

In this case, vehicle i will leverage ω_{ij}, ω_{ik}, and ω_{jk} to estimate its own trustworthiness. For the pair of chosen vehicles j and k, we use p'_j and p'_k to denote the estimated values of p_j and p_k. Assuming $p'_j = p'_k$, from Eq. 6, we can obtain the estimated probability p'_j (or p'_k). Based on the estimated p'_j, i will obtain an estimated p'_i from ω_{ij}, using Eq. 6. Similarly, based on p'_k, i can get another estimated p'_i from ω_{ik}. Taking the average of obtained p'_i's, we obtain a more accurate estimation of p_i. The same procedure applies to all i's neighbors whose trust values are greater than t^*. Taking the average of all estimated results, we have an estimation of the probability p_i. The estimated probability p'_i is treated as the objective trustworthiness of vehicle i.

Suppose vehicle i wants to evaluate the trustworthiness of vehicle j, it needs to consider three different cases. In the first case, vehicle j already derived its own estimated probability p'_j, then vehicle i simply adopts this probability as j's trust. Because p'_j is actually vehicle j's objective trust, it should be more accurate than i's subjective opinion on j's trust. In the second case, vehicle i may have interactions with j, i.e., ω_{ij} is not empty, but j does not know its own objective trust. In this case, i may obtain an estimation about its own objective trust p_i and then derive an estimation of the objective trust of j. Last but not the least, if vehicle i has no interaction with j, it can only rely on its neighbors' recommendation to derive a subjective opinion of j's trust. In this case, the OpinionWalk algorithm discussed in the previous section will be applied and the computed $E(\Omega_{ij})$ is considered j's trust.

In the first case, direct subjective trust assessment only considers the number of observed objects, not the number of vehicles in the network, so its time complexity is $O(1)$. In the second case, a vehicle needs to check the trust of all its neighbors, so the time complexity could be as big as $O(n)$. In the third case, as OpinionWalk algorithm is executed to compute a vehicle's trust, so the time complexity is $O(n^2)$. Overall, the time complexity of the proposed dynamic trust assessment mechanism is $O(n^2)$.

B. Community-Based Trust Assessment

Although direct interactions could facilitate the trust assessment between vehicles, it is possible that two vehicle have no interactions. Due to the large number of vehicles on road, it is expensive to maintain the network information of a vehicular social network on a central server [9]. This is because vehicles need to frequently upload network changes to the server and the changes must be distributed to all vehicles in real time. It is more practical that vehicles record local/individual social networks on themselves, by keeping track of the data exchanged among them. As a result, only a small-size local vehicular social network is maintained on each vehicle. When vehicles encounter on road, their local social network information, as well as their sensing data, will be shared between each other. In the following subsections, we will explain how local vehicular social networks are maintained on vehicles and how to leverage them to conduct trust assessment in a vehicular social network.

1) Community Detection: Most social networks can be divided into several communities, based on the social connections among users. This phenomenon is also observed in vehicular social networks. For example, vehicles usually move within a certain area along several commonly driven routes; therefore, these vehicles are more likely to meet each other frequently. A "community" of a vehicular social network can be described as a group of vehicles that have more connections between each other but fewer connections to the vehicles in other groups. Given a vehicular social network $G(V, E)$, we can derive a few sub-graphs/communities, denoted as $g(V_i, E_i)$.

There are many community detection algorithms that identify non-overlapping communities in a graph. For most of these algorithms, prior information such as the number and size of communities are needed. However, these information may not be available to individual vehicles. Without these information, we adopt the asynchronous label propagation algorithm [10]. This algorithm can detect communities in a linear time, without knowing the number and size of communities.

Each sub-graph identified by the algorithm is called a community. Within each community, there are strong connections among vehicles, while the connections to vehicles in other communities are weaker. Let's assume node/vehicle A is a member of community $g(V_1, E_1)$. Then, A needs to keep an opinion matrix M_1 to reflect the social connections between all nodes in V_1. It is worth mentioning that nodes in V_1 might also have direct connections to nodes in other communities, we call these connections as out-connections. For these out-connections, the corresponding trust opinions will also be kept in M_1. As M_1 is a group of trust opinions, it will be used to compute the trust between intra-community and inter-community vehicles. On each vehicle, a time stamp is also recorded for each opinion in the matrix to indicate the time instance when the corresponding opinion was created. As a vehicle belongs to only one community, we need to consider the trust computation of inter- and intra-community vehicles.

2) Intra-Community Trust Assessment: Intra-community vehicles will update their social trust networks when the meet, by exchanging their trust opinion matrices. The new matrix on each vehicle needs to reserve the trust network information from both of them. If the information of one edge are different, from the trust matrices provided by these two vehicles, the most-recently opinion will be kept, according to the time stamp information. After the interaction, these two vehicles will have the same trust opinion matrix.

Let's assume vehicles A and C are in the same community but A has only a subjective opinion about the trust of C. Vehicle A needs to search its local social network, or the community where it resides, to find all possible paths from A to C to compute the indirect trust between A and C. If we denote these paths as a set r, it will be a subset of all the paths from A to C in the global social network. Here, we use r to estimate the indirect trust of C, from A's perspective.

As show in Fig. 4, we can see that the paths in R_1 and R_2 are derived from A's local trust opinion matrix and they

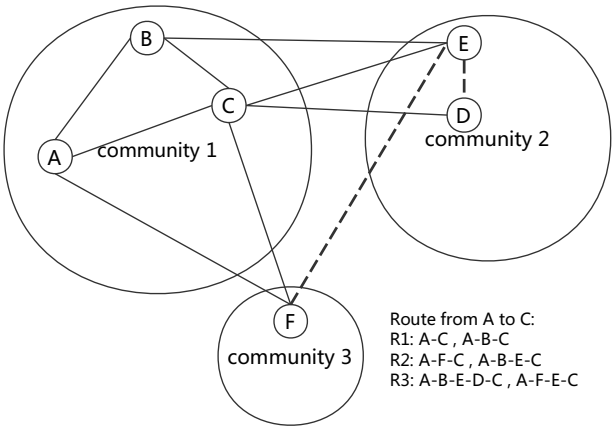


Fig. 4. Possible paths between intra-community nodes.

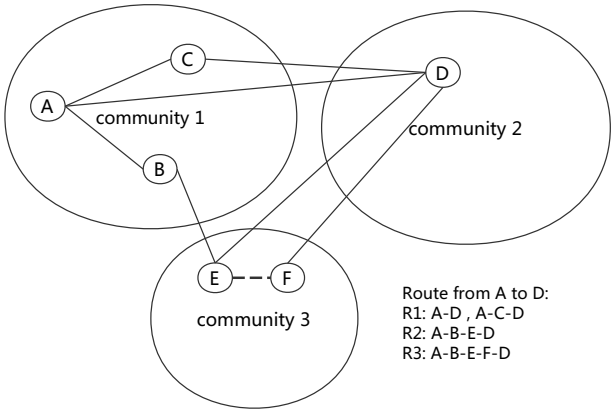


Fig. 5. Possible paths between two inter-community nodes.

are all in r. Although the paths in R_2 involve nodes from other communities, e.g., node F in community 3, the paths can be obtained since A records all its out-connections in its trust opinion matrix. The paths in R_3, however, will be lost in trust computation as the trust opinions ω_{FE}, ω_{ED} will not be available to A. We note that all paths in R_3 have more than three hops from A to C. Based on our previous study [4], paths longer than two hops would not significantly affect trust assessment. In addition, due to fact that nodes tend to strongly connect to intra-community nodes, the out-connections and paths like R_3 are not common in practice.

Notably, it is possible that A cannot always has an accurate assessment on C based of its direct observation. For example, A's sensors are not working properly, or the data collected by A are noisy or not statistically enough. As a result, A needs to take others' assessments into considerations. Therefore, it makes sense that A also needs to assess the indirect trust path(s) between itself and C.

3) Inter-Community Trust Assessment: Similar to the intra-community trust assessment, it is possible to conduct inter-community trust assessment between two vehicles that belong to two different communities. The difference here is that, instead of using only one trust opinion matrix, two opinion matrices from two communities are needed in trust assessment. When two inter-community vehicles encounter with each other, they will exchange data as well as the trust opinion matrices corresponding to their local social networks. As two vehicles come from different communities, we use r to denote the possible paths that are derived from the two trust opinion matrices. From these paths, the indirect trust between these two vehicles can be obtained.

Let's assume vehicle A is a member of community C_1 and D is from community C_2. As show in Fig. 5, not only the paths connecting communities C_1 and C_2 but also that involving node E from community C_3 will be considered in the trust computation. As a result, the paths in R_1 and R_2 will be used to compute A's opinion about D's trust, given A and D are from different communities. Some paths like R_3 will not be detected by checking the trust opinion matrices for communities C_1 and C_2, because it requires the connection information ω_{EF} that is not available to either A or C. As we know, the path like R_3 must be longer than three hops and the trust opinion derived from a long path usually has minor affect on trust assessment. Therefore, the path R_3 is ignored in the trust assessment process.

4) Dynamics of Community: Vehicles may join into different communities at different times for various reasons. For example, a vehicle driven by a professor will be a member of the community composed of vehicles driven by other professors in a university during weekdays. The vehicle might, however, join into the community of drivers who often play golfs in the weekends. Therefore, some vehicles may switch between different communities. In other words, vehicles should change its home community to which it belongs, when necessary.

Let's assume vehicle A is in community C_1 and it receives a piece of data from another vehicle in community C_2. We denote C_1 as node A's home community and C_2 the foreign community. A vehicle may have more than one foreign communities but only one home community. Here, we are interested in how to dynamically adjust a vehicle's home community to facilitate accurate trust assessment. In the above example, vehicle A will take a four-step procedure to determine its home community. First, A finds all nodes it connects to in its current home community C_1, which is denoted as N_A^h where N stands for the neighboring nodes of A. Second, A will find all nodes it connects to in its foreign community C_2, denoted as N_A^f. Third, A needs to know which vehicle(s) it recently frequently interact with, i.e., it records the vehicles it connects to, no matter they are from A's home community or foreign community, within a certain time period of t. The set of nodes is denoted as N_A^t. All vehicles in N_A^t must have derive a new trust opinion of A recently. Fourth, the following opinions will be identified, i.e., ω_{AB_i} (B_i is a vehicle in $N_A^h \wedge N_A^t$) and ω_{AB_j} (B_j is in $N_A^f \wedge N_A^t$). These opinions will be combined and compared to determine whether A is

associated with C_1 or C_2

$$\frac{\left|\{\omega_{AB_i}\}\right|}{\left|\{\omega_{AB_j}\}\right|}, \tag{7}$$

where $|\cdot|$ stands for the cardinality of a set. If the ratio is smaller than a certain value, it implies A is not as connected to C_1 as it to C_2, so A's home community needs to be changed to C_2 in this case. As a result, the opinion matrix for C_2 will be kept and maintained on A and shared with other vehicles when it encounters with in the future. Otherwise, A will keep its current home community.

If the ratio is smaller, it means A recently interacted with more vehicles from C_2. As a result, vehicles in C_2 will update their opinions about A's trust in their trust opinion matrices. On the other hand, vehicles in community C_1 will not receive any data from A. Their opinions about A's trust becomes stale and will be eventually removed from their trust opinion matrices. That means vehicle A will finally disappear from C_1 and join C_2. As the community-based trust assessment explores vehicle's trustworthiness in individual communities, the time complexity here will be $O(n^2)$.

V. Experiment and Evaluation

For static trust assessment where network topology does not change, we evaluated the performance of OpinionWalk in our previous work [6]. For dynamic trust assessment, we simulate a vehicular network where vehicles exchange data and conduct trustworthiness assessment of each other. The accuracy of the proposed trust assessment mechanism is evaluated in the simulations.

A. Dynamic Trust Assessment

1) Simulations of VSN: To understand the performance of the dynamic trust assessment in a vehicular social network, we develop a simulator that supports data exchanging and trust assessments among vehicles. In the simulator, we randomly deploy 100 vehicles within a 1000x1000 m^2 area. The sensing accuracy of a vehicle is simulated to follow a Gaussian distribution, i.e., $G1 \sim \mathcal{N}(\mu, \sigma^2)$ where $\mu = 0.9$ and $\sigma^2 = 0.1$. In other words, different vehicles have different sensing accuracies. To evaluate whether the proposed solution is able to detect untrustworthy vehicles, we also randomly set 10 vehicles with a lower sensing accuracy ($\mu = 0.3$) in the simulations. Those vehicles may generate incorrect sensing data due to several reasons, e.g., fault sensors, malware infection, incorrect calibration, etc. We take a snapshot of all vehicles in the simulation and show them in Fig. 6. The graph in the figure is essentially a vehicular social network where vehicles are connected if they encountered and exchanged data between each other. We use different colors to depict the objective trust of vehicles, i.e., darker the node's color, higher the trustworthiness. Similarly, the expected belief of the subjective opinion between two nodes is also indicated by different gray levels. Darker the edge means higher the trustworthiness (between two nodes). To simulate the movement of vehicles, we adopt the random waypoint model. Based on the model, a vehicle randomly selects a point in each simulation step and moves to that point in the next step. Although other mobility models, e.g., the car following model, may provide a more accurate simulation of vehicles' movement, we believe similar results will be obtained.

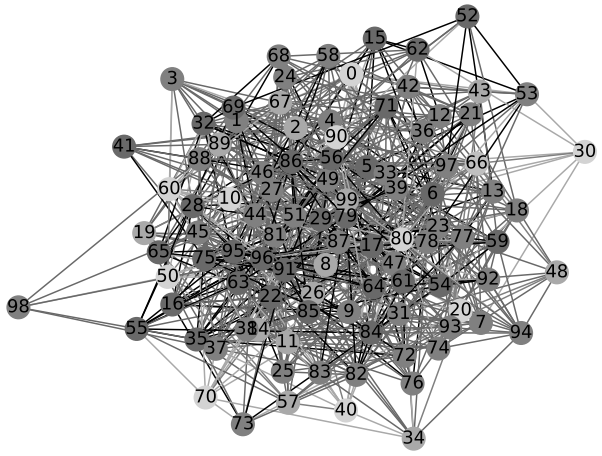


Fig. 6. A snapshot of the vehicular social network in simulations.

In the simulations, we set the communication range of a vehicle as $5m$. Once a vehicle is in the communication range of another one, an interaction occurs and an edge is added/updated in their local social networks. As a vehicle can only verify the data it received, based on its own observation, there will be errors in its trust assessment. Based on $G1$, a vehicle's sensing accuracy can be obtained. We use b to denote this accuracy value. When a vehicle generates sensing data, we assume the accuracy of the data also follows a Gaussian distribution, $G2 \sim \mathcal{N}(b, \sigma_1^2)$ where $\sigma_1^2 = 0.001$. With Eq. 6, the vehicle can build a subjective opinion about the trust of another vehicle. If these two vehicles never meet before or their previous interactions are too old to be useful, we will add a new edge with the computed subjective opinion into the trust opinion matrices on these vehicles. Otherwise, the computed subjective opinion will be combined with the existing opinion in the trust opinion matrices to derive a new one.

2) Accuracy of Objective Trust Assessment: In the section, we periodically measure the errors of direct objective trust assessment of every vehicle in the network. The estimated objective trust value is compared with the ground truth, i.e., the sensing accuracy of each vehicle, then the absolute errors are plotted in Fig. 7. In the figure, we also show the number of edges within the underlying vehicular social network when the simulation time increases from 0 to $25,000s$. We can see that when more interactions occurred among vehicles, more edges are added into the network, offering opportunities for accurate objective trust assessment. Therefore, the average error of estimated objective trust becomes smaller and smaller. In the figure, we find the error of objective trust assessment becomes stable after $4000s$, when 3500 edges are added into the network.

However, as mentioned above, the estimated objective trust value is not the sensing accuracy of a vehicle. This is because

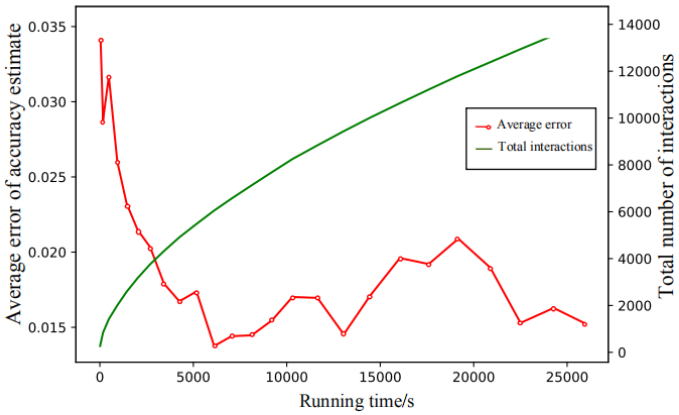


Fig. 7. Average error of objective trustworthiness assessment.

the estimated value will be impacted by the variance of $G2$. It is worth mentioning that once σ^2 is larger than a certain value, the estimated error may become larger as the network evolves.

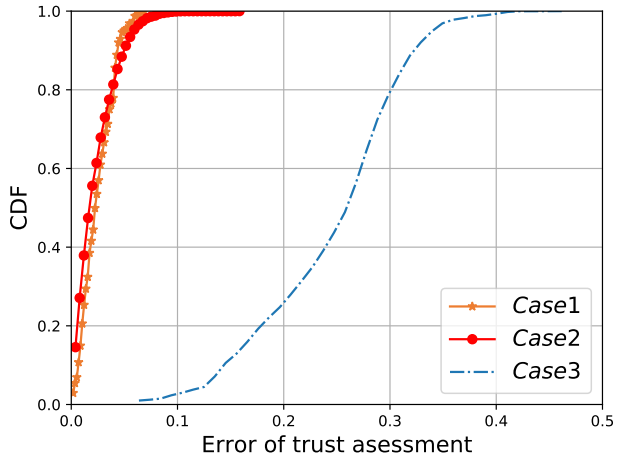


Fig. 8. Error of subjective and objective trustworthiness assessment.

As discussed in Section IV, a vehicle is able to estimate the trustworthiness of another vehicle in three different cases. In case 1, a trustor vehicle derives its own trustworthiness if it has more than two trustworthy neighbors. In case 2, the trustor and trustee vehicles exchanged data between each other, and the trustor vehicle can make a good estimation about the objective trustworthiness of the trustee vehicle. In case 3, the trustor and trustee vehicles have no interaction and only subjective trust of the trustee vehicle can be obtained. In this case, the OpinionWalk algorithm is used to estimate the subjective trust of all vehicles in the trustor vehicle's local social network. As shown in Fig. 8, we found the interactions between vehicles play a vital role in trust assessment as they enable more accurate objective trust estimation (case 1 and 2), compared to the subjective trust assessment (case 3).

3) Impact of Community Division: In this section, we divide vehicles into three communities in the simulations, as shown in Fig. 9. The trustworthiness of vehicles and the trust relations between vehicles are also indicated by different colors, i.e., darker the color, higher the trust. In the simulations, three groups of vehicles move within three non-overlapping regions.

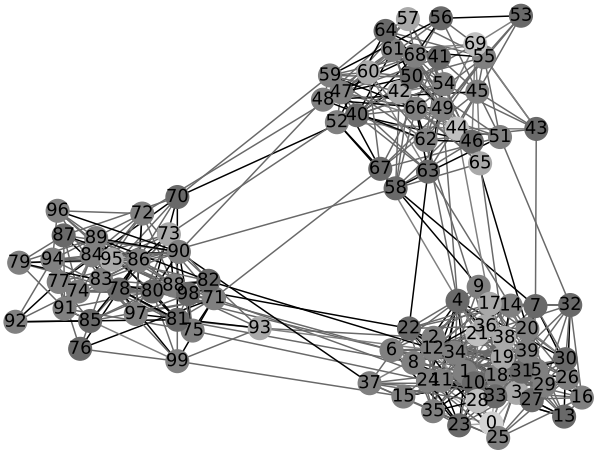


Fig. 9. A snapshot of the vehicular social network composed of three non-overlapping communities.

Particularly, we configure the vehicle's mobility model as follows: a vehicle connects to another intra-community vehicle with a probability of 0.2, and to an inter-community vehicle with a probability of 0.02. To simulate the cases when a vehicle moves from a community to another one, we allow a vehicle to leave its home community to join in another one with the probability of 0.01. As a result, we denote the global vehicular social network as G and the local social network in a community as g. Given a vehicular social network, no matter it is in G or g, we are able conduct trust assessment of vehicles in the network. The difference is that some edges/connections between vehicles in G may disappear in g, which may cause errors in trust estimation. However, the loss of some edges in g offers a better system performance and scalability. In Fig. 10, we compare the error of trust assessment when community division is enabled. As we can see, the errors of trust assessment in cases 1 and 2 are similar, when G and g are used. The error is about 5% larger in case 3, if g is used to assess trust, instead of G. This is because the loss of some important paths in computing the subjective trustworthiness of a trustee vehicle may affect the trust assessment results.

Although the community division technique causes a loss in trust assessment, it substantially reduces the time needed for trust assessment. Here, we are only interested in the case 3 where a trustor vehicle tries to assess the subjective indirect trust of the trustee vehicles, based on other vehicles' recommendations. As shown in Fig. 11, we set the number of vehicles in each community as 60 and increase the number of communities to $3, 5, 8$, and 12. As a result, the total number of vehicles increases to $180, 300, 480$, and 720, respectively. As we can see, with the increase of the number of communities,

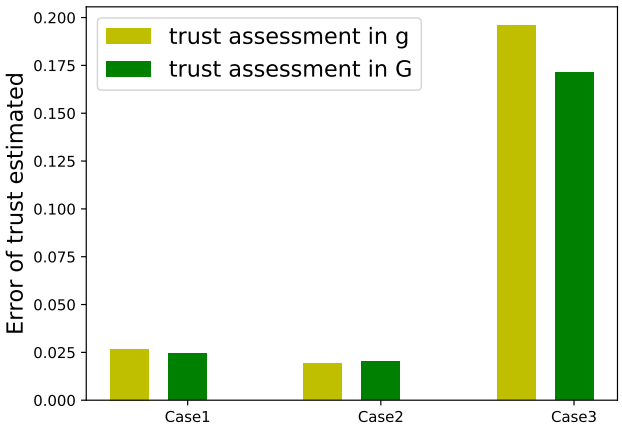


Fig. 10. Error of trustworthiness assessment with community division.

the average execution time for trust assessment drastically increases. On the other hand, if trust assessment is conducted within communities, the average execution time of trust assessment slowly increases.

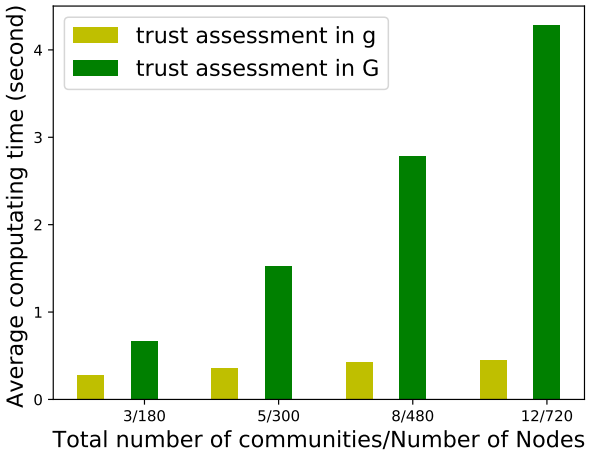


Fig. 11. Execution times of trust assessment w/ and w/o community division.

VI. Related Work

Although Public Key Infrastructure (PKI) secures and authenticates vehicles in vehicular networks [11], it offers only the identification of vehicles but not the trustworthiness of data exchanged among vehicles [12].

A. Vehicular Social Network

Traditional research on vehicular network focuses mainly on efficient data communications [13]–[17] and location privacy protection [18]–[20], however, there is not adequate study on information trustworthiness in a vehicular network. Recently, a social network approach to study information trustworthiness in vehicular ad hoc network (VANETs) has attracted lots of attentions [21], [22]. The basic idea is to leverage how human perceive trustworthiness in received information to achieve trustworthy information sharing between vehicles. It worth mentioning that social trust has already been applied in the wireless network domains. For example, social trust is applied in cellular network to facilitate energy efficient collaboration for video distribution among mobile users [23]. Most recently, the trust relationships between participants are considered to achieve better data privacy protection in mobile crowd-sensing [24]. These research efforts implies social trust plays a vital role in data sharing among mobile devices, and it is critical to study the trust issue in vehicular social networks.

The terminology vehicular social network (VSN) was first introduced in [25] where VSN connects drivers who are physically close to each others, enabling them to take advantage of their close proximity to form a tightly-coupled, ad-hoc, and virtual world. In such a social network, vehicles can form a number of small communities that mirror and facilitate real-world interactions. VSN will become a popular mobile social network primarily because it directly takes advantage of the physical locality patterns of vehicles to enhance opportunities of socialization among vehicles. In weekdays, most people spend hours on commuting between their homes and offices; in weekends, people usually drive on regular routes, e.g. grocery shopping in particular stores. If people travel along similar routes at similar times on every day, it is possible to construct a periodic virtual social network among them. The interactions between them, e.g. sharing information and notifying warnings, will create the opportunity of learning trust relationship between vehicles and then make trustworthy information sharing in VSN possible [26].

Although trust is an extremely important concept in human's life, unfortunately, there is no formal definition of trust. However, most researchers agree that trust is "the willingness of accepting vulnerability or risk based on expectations regarding another person's behavior [27]." According to this definition, there were some efforts on trust managements in vehicular networks [28]–[30], which studied information announcement schemes for VANET based on reputation systems. A message is considered reliable if the sender has a sufficiently high reputation [30]. Trust in VSN is different from trust in online social networks as the entities in VSN are not humans but vehicles/computers. Moreover, trust within VSN is not the same as trust in multi-agent systems [31], [32] where no explicit social structures exist between agents. The fundamental question of trust in VSN remaining unaddressed is: how should a vehicle trust the information sent by others [5].

B. Trust Assessment in Social Networks

Approaches to trust assessment in OSNs can be roughly divided into two broad categories, based upon how trust is modeled. Assuming trust is a real number, researchers studied how to compute relative trust [33], [34] and absolute trust [35], [36] in an OSN. On the other hand, trust can be modeled as a statistical distribution [3], [37]–[40], so more accurate trust assessments are realized.

In the first category, relative trust is first studied in peer-to-peer file-sharing networks [33]. Authors in [33] proposed

the EigenTrust algorithm that starts from a peer and searches for trustworthy peers based on the following rules. It moves from a peer to another with the probability that is proportional to the other peer's trust score, i.e., higher the trust score, higher the moving probability. Therefore, EigenTrust will more likely reach trustworthy peers than untrustworthy ones. Later on, the relative trust of web pages is investigated in [34] to identify spam pages. The TrustRank algorithm proposed in [34] again employs random walk on the network to rank the trustworthiness of web pages. These algorithms, however, only generate trust rankings instead of absolute trust values of peers/pages.

Unlike EigenTrust, MoleTrust [35] proposes a method to compute the trustworthiness of a particular user in a personalized way. While walking through the network, MoleTrust only considers incoming edges with trust scores greater than 0.6 and ignores the others. A user's trust score is computed by averaging all accepted incoming edges weighted by the trust scores of the users from whom the edges orientate. Similarly, TidalTrust [36] recursively searches the network with a weighted average approach. The difference between TidalTrust and MoleTrust is that TidalTrust uses only the path(s) with the highest trust score(s), however, MoleTrust considers all paths, as long as the trust score of each edge along the paths is greater than 0.6. Recently, the evolution or dynamics of trust in OSNs is studied in FluidRating [41]. FluidRating uses fluid dynamics theory to understand the evolution of trust in OSNs.

In the second category, trust is modeled as a statistical distribution, e.g., in subjective logic [37], [38], CertProp [39] and three-valued subjective logic [3]. In this way, trust propagation and fusion are treated as the multiplication and summation of statistical distributions. Comparing to solutions in the first category, these works achieve a higher accuracy in trust assessments. However, they have difficulty in handling complex networks due to the limitations identified in [3]. To enable trust assessment over large-scale networks, the AssessTrust algorithm is proposed in [3]. A major limitation of AssessTrust is that it is designed to compute the trustworthiness of one trustee and thus is very slow and inefficient.

VII. Conclusions

Considering the social connections among vehicles allows one to investigate the trustworthiness of individual vehicles, based on the strength of their connections. Frequent and high-quality interactions between vehicles usually indicate strong trust relations, while the trust relations among vehicles aid the subjective indirect trust assessment. To improve the system performance, we further design a community based technique to support intra- and inter-community trust assessment. The distributed solution to trust assessment in a vehicular social network is found to be effective and efficient in simulations. The resulting trust assessment error is as low as 0.025 and the time needed for trust assessment slowly increases as the number of vehicles increases in the network. We will use real-world vehicle trace files and commercial simulators, e.g., SUMO, to further evaluate the performance of the proposed solution in the future.

Acknowledgment

The authors would like to thank National Science Foundation (NSF) for supporting the work through grant NSF CNS-1761641.

References

[1] Z. Su, Y. Hui, and T. H. Luan, "Distributed task allocation to enable collaborative autonomous driving with network softwarization," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2175–2189, 2018.

[2] A. Mai and D. Schlesinger, "Connected vehicles: Service providers at a crossroads," *Cisco Internet Business Solutions Group*, 2011.

[3] G. Liu, Q. Yang, H. Wang, X. Lin, and M. Wittie, "Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic," in *INFOCOM, 2014 Proceedings IEEE*, April 2014, pp. 1698–1706.

[4] G. Liu, Q. Yang, H. Wang, S. Wu, and M. P. Wittie, "Uncovering the mystery of trust in an online social network," in *Communications and Network Security (CNS), 2015 IEEE Conference on*. IEEE, 2015, pp. 488–496.

[5] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 42–47, 2015.

[6] G. Liu, Q. Chen, Q. Yang, B. Zhu, H. Wang, and W. Wang, "Opinionwalk: An efficient solution to massive trust assessment in online social networks," in *INFOCOM 2017-IEEE Conference on Computer Communications, IEEE*. IEEE, 2017, pp. 1–9.

[7] Y. Wang and M. P. Singh, "Formal trust model for multiagent systems." in *IJCAI*, vol. 7, 2007, pp. 1551–1556.

[8] A. Geiger, P. Lenz, and R. Urtasun, "Are we ready for autonomous driving? the kitti vision benchmark suite," in *Conference on Computer Vision and Pattern Recognition (CVPR)*, 2012.

[9] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, 2016.

[10] R. A. Raghavan, Usha Nandini and S. Kumara, "Near linear time algorithm to detect community structures in large-scale networks," *Physical Review E*.

[11] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds," in *Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on*. IEEE, 2012, pp. 370–375.

[12] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[13] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: A content-centric framework," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 60–66, 2017.

[14] J. Almeida, M. Alam, J. Ferreira, and A. S. Oliveira, "Mitigating adjacent channel interference in vehicular communication systems," *Digital Communications and Networks*, vol. 2, no. 2, pp. 57–64, 2016.

[15] S. Gao, A. Lim, and D. Bevly, "An empirical study of dsrc v2v performance in truck platooning scenarios," *Digital Communications and Networks*, vol. 2, no. 4, pp. 233–244, 2016.

[16] X. Wang, C. Wang, G. Cui, and Q. Yang, "Practical link duration prediction model in vehicular ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 3, p. 216934, 2015.

[17] Q. Xu, Z. Su, Q. Zheng, M. Luo, B. Dong, and K. Zhang, "Game theoretical secure caching scheme in multi-homing edge computing-enabled heterogeneous networks," *IEEE Internet of Things Journal*, 2018.

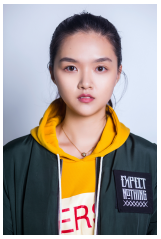
[18] Z. Ren, W. Li, and Q. Yang, "Location verification for vanets routing," in *Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on*. IEEE, 2009, pp. 141–146.

[19] Q. Yang, A. Lim, X. Ruan, and X. Qin, "Location privacy protection in contention based forwarding for vanets," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–5.

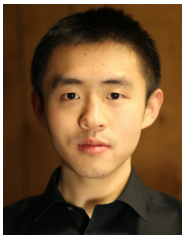
[20] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, 2018.

[21] D. Huang, Z. Zhou, X. Hong, and M. Gerla, "Establishing email-based social network trust for vehicular networks," in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. IEEE, 2010, pp. 1–5.

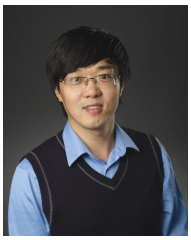
[22] X. Lin, R. Lu, X. Liang, and X. Shen, "Stap: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 2147–2155.
[23] D. Wu, Q. Liu, H. Wang, D. Wu, and R. Wang, "Socially aware energy-efficient mobile edge collaboration for video distribution," *IEEE Transactions on Multimedia*, vol. 19, no. 10, pp. 2197–2209, 2017.
[24] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet of Things Journal*, 2017.
[25] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "Roadspeak: enabling voice chat on roadways using vehicular social networks," in *Proceedings of the 1st Workshop on Social Network Systems*. ACM, 2008, pp. 43–48.
[26] X. Li, Q. Yang, X. Lin, S. Wu, and M. Wittie, "Itrust: interpersonal trust measurements from social interactions," *IEEE Network*, vol. 30, no. 4, pp. 54–58, 2016.
[27] R. Borum, "The science of interpersonal trust," 2010.
[28] F. Dotzer, L. Fischer, and P. Magiera, "Vars: A vehicle ad-hoc network reputation system," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*. IEEE, 2005, pp. 454–456.
[29] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," *International Journal of Computational Intelligence: Theory and Practice (IJCITP)*, vol. 5, no. 1, pp. 03–15, 2010.
[30] D. Huang, X. Hong, and M. Gerla, "Situation-aware trust architecture for vehicular networks," *IEEE Communications Magazine*, vol. 48, no. 11, 2010.
[31] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, no. 1, pp. 1–25, 2004.
[32] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.
[33] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International Conference on World Wide Web*. New York, NY, USA: ACM, 2003, pp. 640–651.
[34] Z. Gyöngyi, H. Garcia-Molina, and J. Pedersen, "Combating web spam with trustrank," in *VLDB '04*, 2004, pp. 576–587.
[35] P. Massa and P. Avesani, "Controversial users demand local trust metrics: An experimental study on epinions. com community," in *Proceedings of the National Conference on artificial Intelligence*, vol. 20, no. 1, 2005, p. 121.
[36] J. Golbeck, J. Hendler *et al.*, "Filmtrust: Movie recommendations using trust in web-based social networks," in *IEEE CCNC*, 2006, pp. 282–286.
[37] A. Jøsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Proceedings of the 29th Australasian Computer Science Conference*, 2006, pp. 85–94.
[38] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 09, no. 03, pp. 279–311, 2001.
[39] C.-W. Hang, Y. Wang, and M. P. Singh, "Operators for propagating trust and their evaluation in social networks," in *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems*, 2009, pp. 1025–1032.
[40] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong, "A trust-based probabilistic recommendation model for social networks," *Journal of Network and Computer Applications*, vol. 55, pp. 59–67, 2015.
[41] W. Jiang, J. Wu, G. Wang, and H. Zheng, "Fluidrating: A time-evolving rating scheme in trust-based recommendation systems using fluid dynamics," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 1707–1715.



Tong Cheng is a visiting graduate student in the Department of Computer Science and Engineering at University of North Texas, Denton, TX, USA. She earned her Master's degree in Computer Science and Technology from Harbin Engineering University, China. She received her bachelor's degree in information security also from Harbin Engineering University in 2016. Her research interests including trust assessment, social network and industrial control.



Guangchi Liu is currently a research scientist in the research & development department of Stratifyd, Inc., Charlotte, NC, USA. He received his Ph.D. in Computer Science from Montana State University, USA. His research interests include Internet of things, trust assessment, social network, and wireless sensor network.



Qing Yang is an assistant professor in the Department of Computer Science and Engineering at University of North Texas, Denton, TX, USA. He received B.S. and M.S. degrees in Computer Science from Nankai University and Harbin Institute of Technology, China, in 2003 and 2005, respectively. He received his Ph.D degree in Computer Science from Auburn University in 2011. His research interests include Internet of Things, vehicular network, network security and privacy. He serves as an Associate Editor of Security and Communication Networks journal.

Jianguo Sun received his B.S. in Computer Science and Technology in 2003, M.Eng in Computer Science and Technology from Harbin Institute of Technology in 2005, and Ph.D. degree in Computer Science and Technology from Harbin Engineering University in 2009, respectively. During 2015 and 2016, Prof. Prof. Sun spent one year at UC Berkeley as a Visiting Scholar. Currently, he is an Associate Dean at the College of Computer Science, Harbin Engineering University, China.